UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

INFORMATION ASSOCIATED WITH THE CELLULAR TELEPHONE ASSIGNED CALL NUMBER 314-599-1814 THAT IS STORED AT PREMISES CONTROLLED BY SPRINT SPECTRUM

Case No. 4:19 MJ 7383 SPM

APPLICATION FOR A SEARCH WARRANT

I, David Herr, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

SEE ATTACHMENT A

located in the _____ District of KANSAS, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18, USC, § 2113	Bank Robbery

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent David Herr
Federal Bureau of Investigation (FBI)

Printed name and title

Sworn to before me and signed in my presence.

Date: 9/20/2019

Judge's signature

City and state: St. Louis, MO

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge

Printed name and title

AUSA: Edward L. Dowd, III

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR TELEPHONE ASSIGNED CALL NUMBER 314-599-1814 THAT IS STORED AT PREMISES CONTROLLED BY SPRINT SPECTRUM	)	No. 4:19 MJ 7383 SPM
	)	FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Agent David Herr, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 for information associated with a certain cellular telephone assigned call number **314-599-1814**, a SAMSUNG CELL PHONE MODEL SM-G965U, IMEI: 356420092409267 (hereinafter "the **subject phone**"), that is stored at premises controlled by **Sprint Spectrum (**hereinafter "the Provider"), a wireless telephone service provider headquartered at **6480 Sprint Parkway, Overland Park, KS 66251**. The information to be searched is described in the following paragraphs and in Attachment A. The requested warrant would require the Provider to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since 1998. I have received training at the FBI Academy in Quantico, Virginia, in criminal and national security investigative techniques. I am currently assigned to the Violent Crime

Squad in the St. Louis Division and investigate violations of federal criminal law, including carjacking, bank robbery, extortion, kidnapping, interstate transportation of stolen property, and Hobbs Act robberies. I have been the affiant and/or received training on search warrants involving these crimes and related cellular data.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, USC 2113 have been committed, are being committed, and will be committed by Kenny Oneal or other persons known and unknown. There is also probable cause to search the location described in Attachment A for the information described in Attachment B for evidence of these crimes.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO WIRELESS PROVIDERS

6. In my training and experience, I have learned that the Provider is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site

data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (*i.e.*, antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (*i.e.*, faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

7. Based on my training and experience, I know that wireless providers can collect cell-site data about the subject phone. I also know that wireless providers such as typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

8. Based on my training and experience, I know that wireless providers typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information

can be used to identify the subject phone's user or users and may assist in the identification of co-conspirators and/or victims.

9. Because the cellular device generally attempts to communicate with the closest unobstructed tower, by reviewing the above-described information, your affiant and other law enforcement officers can determine the approximate geographic area from which the communication originated or was received.

10. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

11. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service used, the ESN or other unique identifier for the cellular

device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates and times of payments and the means and source of payment (including any credit card or bank account number).

PROBABLE CAUSE

1. The United States is investigating bank robberies. The investigation concerns possible violations of, inter alia, Title 18, USC 2113 (Bank Robbery) by Kenny Oneal and others known and unknown, and for its reasons states as follows:

2. On April 29, 2019 at approximately 5:45 pm, a white male suspect entered the Electro Savings Credit Union, located at 12400 Tesson Ferry Road, in St. Louis, MO within the Eastern District of Missouri. The credit union's surveillance showed the suspect appear to look around the branch for a short period of time, otherwise referred to as "casing" the area, prior to exiting the branch. The suspect's physical description and some of the clothing worn would match that of a suspect during a bank robbery that would take place three days later at the same location.

3. On May 2, 2019, at approximately 5:57 pm, a white, male suspect entered the same Electro Savings Credit Union. The suspect approached the bank employees, withdrew a firearm and announced the robbery. The suspect directed the employees to the rear area of the branch where the vault was located and ordered one of the employees to open the vault, which they did. The suspect stole approximately $142,000 in US Currency belonging to the credit

union. The suspect indicated that there was a bomb placed near the bank that would detonate if anyone used their cellular phones. The suspect took the money and exited the credit union.

4. Through interviews of witnesses and review of the credit union's surveillance video, the following description of the suspect was formulated: white male, approximately 6'0", thin build, mid to late 60's, possibly a fake mustache, and bowed leg(s).

5. On September 12, 2019, at approximately 9:15 am, a white, male suspect entered the Alliance Credit Union, located at 5011 Hampton Avenue in St. Louis, MO, within the Eastern District of Missouri. The suspect approached the bank employees, withdrew a firearm and announced the robbery. The suspect placed a shoebox on the teller counter and removed the lid, exposing what appeared to be and what the suspect referred to as a bomb. The suspect directed the employees behind the teller counter where the vault was located and ordered one of the employees to open the vault, which they did. The suspect stole approximately $128,000 in US Currency belonging to the credit union. The suspect took the money and the shoebox and exited the credit union.

6. Through interviews of witnesses and review of the credit union's surveillance video, the following description of the suspect was formulated: white male, approximately 6'0", thin build, mid to late 60's, possibly a fake mustache/goatee, and bowed leg(s).

7. A neighborhood canvass was performed. A witness who worked within close proximity to the credit union indicated that they spoke to a person who matched the description of the bank robber prior to the robbery on September 12, 2019. The witness further stated that they had asked the suspect to move a smaller blue SUV from in front of their business.

8. A review of Alliance Credit Union's exterior cameras was completed. On September 12, 2019, at approximately 7:40 am, a blue 2010 Mazda CX-9, with Missouri license

plate "Tokenk," drove through the parking lot of the Alliance Credit Union. That vehicle is registered to Candice and Kenny Oneal, at 5756 Hawkins Fuchs Road in St. Louis, MO, within the Eastern District of Missouri. Kenny Oneal's ("Oneal") Department of Revenue Driver's License photograph and information is similar in description to that of the suspected bank robber.

9. On September 12, 2019, your affiant conducted physical surveillance of Oneal's residence and witnessed Oneal walking to the house through an open garage door. Oneal's physical description matched the suspected bank robber. In addition, a blue 2010 Mazda CX-9 with Missouri license plate "Tokenk" was parked in the garage.

10. On September 13, 2019, investigators made contact with Oneal at his residence. Oneal agreed to allow investigators to enter the residence. Oneal was informed that he matched the description of an individual who had robbed a Credit Union the prior day. Oneal was also informed that his blue, 2010 Mazda CX-9, with Missouri plate "Tokenk" appeared to have been used by the robber. Kenny Oneal agreed to show investigators his vehicle, which was parked in the garage of the residence. Photographs were then taken of the vehicle.

11. Investigators again noticed several physical characteristics of Oneal which matched the robber, including his bowed leg(s), facial features, etc. At that time, detectives from the St. Louis Metropolitan Police Department ("SLMPD") placed Oneal into custody. Oneal directed investigators to a room in the basement in order to change clothes. The **subject phone** was located near the bed and Oneal informed investigators that the **subject phone** belonged to him. Oneal was conveyed to the SLMPD South Patrol. While at South Patrol, the **subject phone** rang and the phone number "314-249-8508" showed on the screen. That number was later

determined to belong to an associate, by the name of "J.F." Investigators were informed that Oneal was not at his house at the time of the robbery, but was with J.F.

12. On September 13, 2019, contact was made with J.F. who denied being with Oneal the day prior. To confirm this, J.F. showed investigators text messages from Oneal. Oneal is listed in J.F.'s phone as "Sundance Kid" at telephone # 314-599-1814, the same number as the **subject phone**. A message on J.F.'s phone was received on September 12, 2019 at approximately 9:45 am, which was approximately 30 minutes after the robbery. The message requests J.F. to provide an alibi for Oneal's whereabouts for the morning of September 12, 2019 and then to delete all text messages between the two parties. A review of the call log on J.F.'s phone confirmed that he had attempted to contact Oneal the morning of September 13, 2019.

13. The **subject phone** is currently in the lawful possession of the St. Louis Division of the Federal Bureau of Investigation (hereinafter the "investigative agency(ies)").

12. On September 17, 2019 the United States sent preservation letters pursuant to 18 U.S.C. § 2703(f) to Sprint that requested the providers preserve the data identified in Attachment A.

AUTHORIZATION REQUEST
INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

13. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41. The United States will execute this warrant by serving the warrant on the Provider. Because the warrant will be served on the Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

14. I further request that the Court direct the Provider to disclose to the United States any information described in Section I of Attachment B that is within its possession, custody, or control.

CONCLUSION

15. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,

DAVID HERR
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on Sept. 20, 2019

SHIRLEY P. MENSAH
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number **314-599-1814**, a SAMSUNG CELL PHONE MODEL SM-G965U, IMEI: 356420092409267 ("the Account"), that are stored at premises controlled Sprint Spectrum ("the Provider"), headquartered at **6480 Sprint Parkway, Overland Park, KS 66251**.

Attachment B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period **April 1, 2019 – September 13, 2019**:

a. The following information about the customers or subscribers of the Account:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received as well as per-call measurement data (also known as the "real-time tool" or "RTT" data).

The Provider is hereby ordered to disclose the above information to the government within 14 days of the date of this warrant.

II. Information to be Seized by the United States

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of **Title 18 U.S.C. Section 2113** involving **Kenny Oneal** during the period of **April 1, 2019 – September 13, 2019**.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are

authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by SPRINT SPECTRUM, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of SPRINT SPECTRUM. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **SPRINT SPECTRUM**, and they were made by **SPRINT SPECTRUM** as a regular practice; and

b. such records were generated by **SPRINT SPECTRUM** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **SPRINT SPECTRUM** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **SPRINT SPECTRUM**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature